ARTICLE INFO
Article ID: 12-07-02-0013

doi:10.4271/12-07-02-0013

A Global Survey of Standardization and Industry Practices of Automotive Cybersecurity Validation and Verification Testing Processes and Tools

Andrew Roberts,[1] Stefan Marksteiner,[2,6] Mujdat Soyturk,[3] Berkay Yaman,[4] and Yi Yang[5]

[1]Tallinn University of Technology, Estonia
[2]AVL List GmbH, Austria
[3]Marmara Üniversitesi, Turkey
[4]BigTRI, Turkey
[5]AVL China, China
[6]Mälardalen University, Sweden

Abstract

The United Nation Economic Commission for Europe (UNECE) Regulation 155—Cybersecurity and Cybersecurity Management System (UN R155) mandates the development of cybersecurity management systems (CSMS) as part of a vehicle's lifecycle. An inherent component of the CSMS is cybersecurity risk management and assessment. Validation and verification testing is a key activity for measuring the effectiveness of risk management, and it is mandated by UN R155 for type approval. Due to the focus of R155 and its suggested implementation guideline, ISO/SAE 21434:2021—Road Vehicle Cybersecurity Engineering, mainly centering on the alignment of cybersecurity risk management to the vehicle development lifecycle, there is a gap in knowledge of proscribed activities for validation and verification testing. This research provides guidance on automotive cybersecurity testing and verification by providing an overview of the state-of-the-art in relevant automotive standards, outlining their transposition into national regulation and the currently used processes and tools in the automotive industry. Through engagement with state-of-the-art literature and workshops and surveys with industry groups, our study found that national regulatory authorities are moving to enshrine UN R155 as part of their vehicle regulations, with differences of implementation based on regulatory culture and pre-existing approaches to vehicle regulation. Validation and verification testing is developing aligned to UN R155 and ISO21434:2021; however, the testing approaches currently used within industry utilize elements of traditional enterprise information technology methods for penetration testing and toolsets. Electrical/electronic (E/E) components such as embedded control units (ECUs) are considered the primary testing target; however, connected and autonomous vehicle technologies are increasingly attracting more focus for testing.

History

Received: 07 Mar 2023
Revised: 25 Aug 2023
Accepted: 24 Oct 2023
e-Available: 16 Nov 2023

Keywords

Cybersecurity standards, Validation and verification, Cybersecurity testing, Best Practices

Citation

Roberts, A., Marksteiner, S., Soyturk, M., Yaman, B. et al., "A Global Survey of Standardization and Industry Practices of Automotive Cybersecurity Validation and Verification Testing Processes and Tools," *SAE Int. J. of CAV* 7(2):2024, doi:10.4271/12-07-02-0013.

ISSN: 2574-0741
e-ISSN: 2574-075X

1. Introduction

UNECE's regulation 155 (UN R155) [1] requires a structured approach to cybersecurity engineering of automotive systems, using a cybersecurity management system. This regulation is mandatory for compliance with automotive type approval within many of the most important automotive markets including Europe, Korea, and Japan. Without compliance to the UN R155, original equipment manufacturers (OEMs) may currently not commission new models, and, from mid-2024, will be restricted from selling to these markets. Therefore, OEMs are motivated to comply with this regulation due to the financial risk of losing market access due to noncompliance. Closely related to UN R155 is the ISO/SAE 21434:2021—Road Vehicles—Cybersecurity engineering, which is commonly accepted as the guiding standard for automotive cybersecurity [2]. UN R155 requires automotive manufacturers to have for their automotive product a Cybersecurity Management System (CSMS). The ISO/SAE 21434:2021 provides, so far, the only global standardized approach for development of an automotive CSMS (however, it is not explicitly mandatory that a CSMS follows that standard). UN R155 and ISO/SAE 21434:2021 require the structured measures to be verified and documented in a comprehensible and replicable manner using structured testing procedures. However, the details of how to conduct testing applicable to the requirements of UN R155 for type approval and to the standard expected for automotive risk management are mainly left to technical services, vendors, and suppliers. The global standards (including ISO/SAE 21434:2021) only recommend testing methodologies at a very high level (i.e., functional testing, vulnerability scanning, fuzz testing, penetration testing), and provide suggestions for test targets (e.g., checking for exposed debug interfaces, the presence of a secure boot mechanism, usage of encryption in communications, etc.). The complexity of vehicular systems, in conjunction with a diverse ecosystem of standards and procedures make it infeasible to define a solid, standardized testing procedure that spans over the whole (in-homogeneous) system and over the whole life cycle. The development of standardized processes is further challenged, as each large OEM has its own established procedures and guidelines, partially stemming from internal design and coding guidelines as well as from procedures from adjacent domains such as functional safety testing. There also exists a lack of literature that explores the state-of-the-art of automotive cybersecurity testing and how the global standards are being implemented regionally and how industry is developing its cybersecurity testing programs. To confront these challenges, the main idea of this research is to provide a starting point on identifying test targets and testing methods from a global and regional perspective, as well as exploring the usage and applicability of such methods currently used in the automotive industry. To this end, the contributions of this research are as follows:

- We conducted a state-of-the-art analysis of automotive validation and verification testing (V&V) for global and regional automotive cybersecurity standards and regulations.
- We conducted a survey of tools and practices commonly used by manufacturers and admission bodies and analyzed the development of cybersecurity test tools and procedures.
- We discussed the findings of the state-of-the-art and survey and analyzed the progress of the adoption of UN R155.

2. Methodology

The initial stage of the study focused on establishing the standards and regulatory environment for V&V testing of key global automotive regions. The central questions used to guide the research were:

- **RQ1** What is the state-of-the-art for automotive cybersecurity V&V standards?
- **RQ2** How have these standardization approaches been transposed to national regulation?
- **RQ3** What are the V&V testing processes, procedures, and tools used by industry?

These questions enable the extrapolation of key areas of interest for automotive cybersecurity V&V:

- Are there variances between regions in the implementation of regulation and national initiative developed to improve V&V testing, and if so, why?
- What are the key trends for V&V testing adopted in industry? What can these trends tell us about the evolving nature of V&V testing to meet technology innovation?

To answer these research questions, analysis was conducted on three data sources (see Table 1): (1) literature from government authorities, industry, and standardization groups, (2) expert knowledge derived from open-format workshops with regional representatives from a global mobility testing industry working group, and (3) an academic literature from key conferences in the automotive cybersecurity field. The purpose of the academic literature review is to provide a brief overview of the key trends as they relate to ISO/SAE 21434:2021.

2.1. Related Work

There have been numerous reviews of automotive cybersecurity standardization during and after the drafting of ISO/SAE 21434:2021 and the UNECE Regulation R155. Macher et al. [3] first review in 2019 found two predominant challenges of standardization of automotive cybersecurity testing. First, the cross-relations between standards, guidance, recommendation, and regulation created a complex environment that was difficult to interpret. Second, select automotive technologies were governed by diverse standards. An example was given of OBD-II interface, which is mentioned in hardware security and certificate standardization documents. However, the

TABLE 1 Data sources for survey of standardization efforts for automotive cybersecurity V&V testing.

Review	Data source
Literature review of national standards and regulations	• Official government documents (legislation, govt. department documents) • Automotive and transportation reports and standardization reports • Academic literature
Industry survey	• Open format workshops with regional representatives from EU, China, Japan, and North America • Written survey with structured questions
Academic survey	• Literature from automotive security research in academia and standardization body journals

certificate standardization was legacy and was written in 2006, at which, advances in hardware security were not apparent. The second standardization review by Schmittner and Macher [4] in 2020 focused on the draft [5] of the ISO/SAE 21434:2021 standard. In addition to lauding the effort to contribute a common framework and language for automotive cybersecurity, shortcomings identified included ambiguity in descriptions of processes and approaches and the difficulty in providing a standardized context for diverse methods, guidelines, and best practices. Schober and Griessnig [6] mapped the cross-relations of automotive cybersecurity regulations (UNECE No. 155 and 156) and standards (ISO/SAE 21434:2021, ISO PAS 5112, ISO 24089). As this study was written at the initial release of ISO/SAE 21434:2021 and before UNECE R155 and 156, the national level initiatives to support innovations for automotive cybersecurity testing were not captured.

3. Global Regional Perspectives on Automotive Product V&V Testing Standardization and Regulation

3.1. Attack Automotive Product V&V Testing Standardization

As a standard released in 2021, ISO/SAE 21434:2021 [7] brings a specification and a framework for cybersecurity risk management in different phases of product lifecycle: concept, development, production, operation, maintenance, and decommissioning of electrical and electronic systems. While covering the whole engineering process of road vehicles' cybersecurity, the standard also mentions cybersecurity testing by emphasizing its importance and providing a high-level guidance. Worth noting, the document doesn't provide a detailed analysis for the testing methodologies, processes, and tools. Further, the standard brings description and distinguishes between the verification and validation. Because of the lack of test-related details in ISO/SAE 21434:2021, WG11 (Cybersecurity working group) under ISO/TC22/SC32 (Committee of Electrical and Electronic Components and General System Aspects) has proposed ISO PWI 8477, which is a new standardization project for automotive cybersecurity verification and validation. This project is intertwined with a second project: "ISO/SAE PWI 8475: Road vehicles—Cybersecurity Assurance Levels (CAL) and Target Attack Feasibility (TAF)," which is targeted to define automotive cybersecurity assurance levels (CALs) and target attack feasibility (TAF), whereby the CALs are focused on engineering assurance and the TAFs are on the expected strength of technical controls. However, there is not yet (as of June 2022) an official standards project, any results are therefore pending. The standards document SAE J3061_202112 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems) [8] contains an appendix regarding the existing security test tools. Another initiative from SAE International, which is in progress, is the J3061-2 (Security Testing Methods) [2]. The document has been issued by the Vehicle Cybersecurity Systems Engineering Committee with the aim of providing a detailed analysis on the security testing methods on both hardware and software.

A global regulation initiative on automotive cybersecurity is brought recently within an addendum to UNECE 1958 treaty (Regulations 141-160), namely UNECE R. 155 [1] and 156 [9] for automotive cybersecurity. These regulations have a direct impact on OEMs and suppliers as the compliance to UNECE's homologation regulations are fundamental for the automotive type approval process and product development for the market. UNECE Regulation No. 155 (–legally binding document ECE/TRANS/WP.29/2020/79 [10]) mandates the installment of a CSMS as defined in ISO/SAE 21434:2021 [7] to ensure an accompanying cybersecurity process to be executed during the automotive system development lifecycle. In the document, the OEM is required to verify the effectiveness of implemented cybersecurity measures by testing and the approval authority shall refuse the type approval if this cannot be demonstrated including the adequateness of the testing procedures themselves. Lastly, the authority by itself shall also verify the effectiveness of security measures by testing, especially concentrating on the high-risk samples. With the increased threads on cybersecurity of automotive systems due to increased complexity and connectivity; there are initiatives brought by the governments for regulation and standardization. It is seen that it is a general tendency by the governments to prepare the industry for the regulations, with guideline documents on how to properly implement and test the cybersecurity mechanisms (e.g., [11] and [12]). While most of the regulation initiatives across the governments regarding the V&V are still in similar phases of preparation; there are some issuances of documents regarding the type approval by the ministries of Korea and China (see subsections Republic of Korea and China under

Section 3.3.1). In the U.S., the government encourages the industry to collaborate with the regulation activities by commenting on the documents published by the agencies. Regarding the standardization, there are two remarkable initiatives brought by the national standardization organizations of China and Japan, which brought some practical standards on cybersecurity testing and verification (see Section 3.3.1).

3.2. Automotive Academic Survey of V&V

Current trends in academic literature focus on the following areas:

- Novel vulnerability testing of intelligent vehicular technologies and autonomous, self-driving control algorithms.
- Methods for automating cybersecurity testing.

Novel attacks on intelligent vehicular and self-driving technologies focus on the advanced hardware technologies that support perception (LiDAR, camera, radar), localization (LiDAR, GNSS), and vehicular communication [vehicle-to-vehicle (V2V), vehicle-to-infrastructure (v2x)]. Testing is predominantly conducted in high-fidelity digital twin simulation environments and progressively, real-world environments and proving grounds. Tools common in testing of these systems include adversarial neural networks that generate malicious robust physical invariants to perturb object detection and semantic segmentation, fuzzers for protocol vulnerability assessment [13, 14], and, in intelligent vehicles, to send malicious unsanitized sensor telemetry input to impact LiDAR [1, 15], radar, and inertial measurement sensors [16, 17]. White-box testing tends to be more popular for testing of neural networks due to the complexity of understanding the impact of attacks of black-box testing and to optimize testing based on knowledge of the learning model. Automation of cybersecurity testing has focused on aligning fuzz testing techniques with contemporary software development processes. Fuzzing approaches are being developed, which incorporate guidance of the ISO/SAE DIS 21434 to utilize threat and risk assessment (TARA) and cybersecurity assurance levels (CALs) to systematically identify and prioritize attack vectors [18]. Novel methods for testing are being explored on digital twin, digital replications of embedded systems, to understand attack vectors and resultant impacts in a safe, and repeatable and agile test environment [19, 20].

3.3. National Regulatory and Standardization Approaches for Automotive Product V&V Testing

Each signatory of UNECE R155 is required to transpose this regulation into national legislation. As approaches to cybersecurity testing of critical infrastructure differ it is important to understand how national governments are transposing UNECE R155 into their respective ecosystems and how they are supporting the introduction of regulations with initiatives to assist industry and authorities. It is also observed that, despite China is not a contracting party of the UNECE WP.29 1958 Agreement [21] (hence not obliged to follow UNECE R155); the national government perform similar activities referring to ISO/SAE 21434:2021. In North America, situation is different due to the performed system of self-assessment in that region. Despite this, there are national activities with respect to ISO/SAE 21434:2021.

To elucidate this, two components of national approaches to automotive cybersecurity testing are analyzed: (1) governance and implementation of regulation and ISO21434:2021 and (2) national initiatives with regard to automotive V&V testing.

3.3.1. Asia

China

Governance and Implementation of Regulation and ISO/SAE 21434:2021 The Chinese market has seen an emergence of self-driving and interconnected technologies for vehicles. Due to this, the Chinese government ministries are focused on developing policies for cybersecurity and data security of intelligent and connected vehicles (ICVs). To support these policies, corresponding standards committees are developing national standards, of which the majority still are in draft version. In particular, three ministries work in the field of cybersecurity and data security of ICV: the Ministry of Industry and Information Technology (MIIT) and Cyberspace Administration of China (also called Office of the Central Cyberspace Affairs Commission), and the Ministry of Natural Resources.

In late 2021, the MIIT has published two notices [22, 23] to address the security requirement of connected vehicles. In these notices, it mandates that both cybersecurity and data security of connected vehicle must be fully considered before going to market. Building a complete vehicular security standard system is also prescribed to all subdepartments, organizations, and companies. Meanwhile, a mandatory standard for vehicle cybersecurity and technical requirements for vehicle cybersecurity has been issued [24]. Furthermore, ISO/SAE 21434:2021 is being converted to Chinese national standards as well.

National Initiatives With Regard to Automotive Product V&V Testing For general technical security requirements, the National Information Security Standardization Technical Committee (NISSTC) released GB/T 40861-2021 [25] on October of 2021, which involved the security of software, electrical and electronic hardware, data, onboard communication, and V2X communication. Furthermore, the authenticity, confidentiality, integrity, availability, access control, anti-repudiation, auditability, and preventability should be considered to the corresponding

security system, if applicable. Compared to other standards, this standard provides a more complete technical requirement of in-vehicle security. Some standards released by NISSTC focus on the technical requirements as well as test methods of specified system and component. Standard GB/T 41578-2022 [26] addresses in-vehicle charging system and corresponding communication security. It further specifies detailed test methods at hardware, software, data, and communication aspects. GB/T 40856-2021 [27] concerns the security test methods for hardware, communication, operation system, application, and data. GB/T 40857-2021 [28] addresses hardware, software, communication, and data security for CAN gateway, ethernet gateway, and hybrid gateway. GB/T 40855-2021 [29] involves on-board terminals security, communication security, and platform security in the scope. With regard to different kinds of security, standards also provide a few general best practices for testing. For hardware, this includes checking for exposed debug interfaces and their authentication mechanisms, the disclosure of the PCB wiring and design, and for backdoors. For software, checks for secure boot and software integrity, access control, logging mechanisms, as well as vulnerability scans are recommended. The data should be checked for susceptibility to tampering, confidentiality on export, collecting after user approval, sensitive information protection, effectiveness of its deletion, as well as its security during transmission. Communication links should prove their authentication, integrity confidentiality availability, and non-repudiation.

Japan

Governance and Implementation of Regulation and ISO/SAE 21434:2021 Japanese METI (Ministry and Economy, Trade and Industry) published a document about cybersecurity measures for autonomous vehicles in 2018. This document describes the schedule for implementing ISO/SAE 21434:2021. First, JASPAR (Japan Automotive Software Platform and Architecture) collaborates with other countries to establish the standard while suggesting rules and policies that fit in Japanese automotive environment. While developing ISO/SAE 21434:2021, METI and MLIT (Ministry of Land, Infrastructure, Transport and Tourism) create guidelines that describe requirements to develop and operate automotive vehicles, with some governmental organizations such as JASPAR. Besides, METI creates a more concrete guideline for testing and validation/certification of autonomous vehicles collaborating with organizations in industrial sector such as IPA (Information Processing Agency). Until now, MLIT has published guidelines for requirements of autonomous vehicle development like [30] (Japanese). Also, IPA has published and revised more practical guidelines such as [31]. This guideline includes threat analysis and possible measures in a development cycle, namely management, planning, development, and operation. National standards are determined by organizations such as JAPSAR, based on the international standards. The national standards describe requirements that the industry must meet in the development process against assumed security threats. Especially, they have formulated evaluation guide for ECU and hardware/software vulnerabilities. JASO TP-15002 guideline is an evaluation guideline for automotive information security analysis. Japan Automotive Software Platform and Architecture (JASPAR) is a collaboration project of engineers from the automotive industry. The aim of JASPAR is [32]: "identify common issues that will be faced in the future in the car electronics sector, and then undertake standardization initiatives aimed at resolving those issues, creating common objectives across the entire automotive industry."

National Initiatives With Regard to Automotive Product V&V Testing The JASPAR project provides reference architectures for secure design of automotive components and verification testing. The standards are focused on areas of cybersecurity of car electronics where there are gaps in other available standards and areas that are a priority for the Japanese automotive industry. These include software-over-the-air updates, ECUs, CAN-FD, secure communication, and vehicular messaging. JASPAR project details a list of standards applicable to cybersecurity testing of automotive products: TD-CST-4—ECU Penetration Testing Guide Version 1.0, ST-CST-1—ECU Vulnerability Test Requirements Ver.1.1, STOTA-09—OTA Software Update Compliance Test Specification OTA Master Ver.1.0, ST-OTA-10—OTA Software Update Compliance Test Specification—Target ECU Ver.1.0 [32].

Republic of Korea

Governance and Implementation of Regulation and ISO/SAE 21434:2021 There are two main actors in Korea for type approval and certification of vehicles Ministry of Land and Infrastructure, Transport (MOLIT) and Korea Automobile Testing & Research Institute (KATRI) [33]. There are two regulations that pertain to the testing and evaluation of automotive:

- Korea Motor Vehicle Safety Standard (KMVSS)—Technical Regulation
- Korea Vehicle Management Act (Self-Certification system and Safety Standards for Motor Vehicles)

In June 2020, MOLIT established the UNECE R155 international standards for automotive cybersecurity as the main content for recommendations for ROK automotive manufactures. The central component being that the automotive manufacturer has a cybersecurity management system (CSMS) and demonstrate that automotive cybersecurity is managed accordingly. To integrate UNECE R155 local laws and regulations will be amended as appropriate [33]. MOLIT plans to issue the Automotive Cybersecurity law and safety/security regulation in 2022. Until that time, they will have published recommendations and guidelines to fill the gap between the practice of automotive company and the requirements imposed by the registration such as Korea Motor Vehicle Safety Standard (KMVSS) and Korea Vehicle Management Act. The approach taken by MOLIT is to ease

the new policy implementation and adoption recommendations step-by-step. Currently, the differences of UN R155 and the ROK implementation are that ROK extends the R155 to their self-certification approval in addition to type approval, manufacturers obligation to report are focused on data sharing between manufacturers, and administrative matters (procedures, document, penalties) and matters relating to type approval (CSMS certification, DETA data sharing) are yet to be included in the implementation [33]. As one of the recommendations, MOLIT announced guidelines for security of autonomous vehicles on December 15, 2020. The guidelines include (1) Ethical Guidelines for Self-Driving Vehicles, (2) Automobile Cybersecurity Guidelines, and (3) Level 4 Autonomous Vehicle Manufacturing/Safety Guidelines, which provide basic directions for ethics and safety [33]. Among that, Automobile Cybersecurity guidelines introduced recommendations for security policy directions so that automobile manufacturers can develop a cybersecurity system in preparation for the implementation of the security standards to be issued in 2022 [34]. The recommendations proposed in the guidelines are the following:

- Security management such as a process for identifying, evaluating, classifying, and managing security threats must be established within the manufacturer's organization and share relevant information.
- Vehicle security threat identification, evaluation, security measures, and sufficient security-related pre-tests must be performed. Note that security measures include cyberattack detection and prevention measures, risk monitoring support measures, data forensics support measures for cyberattack analysis, and the like.

To support the implementation of R155 as part of domestic regulations, MOLIT has planned to implement an Automotive Cybersecurity Support and Response System. This system consists of an automotive cybersecurity committee to coordinate initiatives including the foundation of an automotive security center. The role of the Automotive Cybersecurity Support and Response System is to provide cybersecurity test and evaluation and enforcement support, support the private sector with the development of automotive technologies, provide cybersecurity incident response, and support for the automotive sector [33].

3.3.2. North America

United States of America

Governance and Implementation of Regulation and ISO/SAE 21434:2021 In the U.S., National Highway Traffic Safety Administration (NHTSA) is the responsible entity under the U.S. Department of Transportation (U.S.DOT), which issues Federal Motor Vehicle Safety Standards (FMVSS) to regulate and standardize the requirements for the safety of motor vehicles [35]. The agency undertakes the responsibility of standardization and regulation of automotive cybersecurity in the U.S. while conducting research in order to address the challenges in the area [36]. To provide a comprehensive and systematic standardization and regulation process, the agency involves the industry in the regulation and standardization process by encouraging the formation [37] of Auto-ISAC [38] and receiving comments on the publications/reports that are published by the agency [39]. Currently, there are no standards or regulations for automotive cybersecurity testing and verification, which is brought by the NHTSA. However, in 2016, the agency published a non-binding document describing guidelines and best practices for automotive cybersecurity [40], which is revised in 2020 concerning the ISO/SAE DIS 21434 draft standard and a draft version has been published (2020 draft) [11]. According to the comments brought on the draft, a pre-final version has been released in 2022 [41]. The document refers ISO/SAE 21434:2021 and NIST's Cybersecurity Framework for standardizing the cybersecurity development, maintaining, and testing process.

National Initiatives With Regard to Automotive Product V&V Testing NHTSA conducts multifaceted research on vehicle cybersecurity that leverages NIST's cybersecurity framework [42] and aims to collaborate with the industry to address the challenges in vehicle cybersecurity. NHTSA's best practices documents include recommendations for automotive cybersecurity testing and documentation. Those practices defined in [41] are as follows:

- Cybersecurity testing, including penetration testing should be implemented as a part of the development process.
- Qualified testers who have not been a part of the development process should be included in the testing phases.
- Identified vulnerabilities during cybersecurity testing should be analyzed; the vulnerability and how the vulnerability is managed should be documented.
- All commercial-off-the-shelf and open-source software components used in vehicle ECUs should be evaluated by the manufacturers in order to identify the vulnerabilities.

For addressing the need for effective information sharing across the industry, NHTSA encouraged the formation of the Auto ISAC, a community established by partners from the various domains of the industry. In collaboration with the Alliance of Automobile Manufacturers (Auto Alliance) and the Association of Global Automakers (Global Automakers), the community published a set of best practices documents on automotive cybersecurity [43]. One of these documents, "Security Development Lifecycle," covers the security needs for the development process and distributes the testing process into the phases of development as follows [44]:

i. **Design**: This phase is where a high-level test plan can be constructed, which identifies:
   - The best security verification methods (e.g., design review, manual code review, automated code analysis, component/unit testing, bench and vehicle penetration testing).

- Needed testing tools including special build components and infrastructure support.
- An evidence sheet with details of software, hardware level, date, pass/fail status, notes on failures or unexpected behavior person running the test and approver, and others as necessary.

ii. **Implementation**: Secure implementation requires testing and verification in both hardware and software levels. The methods for ensuring at the hardware level:

- Confirmation reviews or assessments
- Penetration tests

At the software level:

- Code reviews
- Automated code analysis
- Penetration testing

iii. **Testing and Validation:** This part defines the whole process of testing through phases of the development lifecycle:

1. Cybersecurity Testing: The actual testing process is done during the implementation and post-implementation phase, which evaluates the proper working of safeguard mechanisms and identify potential vulnerabilities that leads to residual risk assessments.
2. Internal Cybersecurity Sign-off Process: The sign-off process includes the testing process, which verifies the system is secure enough to withstand the previously assessed threats. This process should include the overall test plan, performed functional tests, penetration tests, source code audits, and so forth.
3. Residual Risk Assessments: Residual risk assessments can be done as a part of the development lifecycle on a periodic basis as the known residual risks evolve over time by the discovery of new attack methods or cost reduction due to newer/cheaper tools.

Canada

Governance and Implementation of Regulation and ISO/SAE 21434:2021 In Transport Canada's Vehicle Cybersecurity Strategy, the Canadian Department of Transport is responsible for monitoring the work of the National Research Council Canada's Automotive and Surface Transportation Centre. The Automotive and Surface Transportation Centre engages in research and testing related to advanced vehicle technologies. Examples include examination of cybersecurity vulnerabilities in connected features, mapping, and connectivity for automated driving. The testing and evaluation of cybersecurity is closely tied to applicable motor vehicle safety and data privacy legislation [45].

National Initiatives With Regard to Automotive Product V&V Testing The Canada Vehicle Cybersecurity Guidance [45] provides technology-neutral and non-prescriptive guiding principles for the incorporation of cybersecurity throughout the vehicle lifecycle. The guidance promotes the importance of international standards such as ISO/SAE 21434:2021 and other related functional safety standards. The guide provides a descriptive overview of the context of cyber-attacks to vehicular systems and in particular that more advanced attacks tend to be associated with "white-hat" cybersecurity research, while real-world, cyber-criminal threat actors make use of the data-driven ecosystem of vehicular technologies to comprise attacks on back-end systems and systems that generate and store telemetry. To this end, the guide recommends the implementation of layered security controls (known as defense-in-depth), privacy protection, and information protection procedures and testing of data security, secure external vehicle communications, identity management and access control, secure software development, secure updates, and the extended vehicle environment. Cybersecurity testing is recommended to be conducted throughout the vehicle lifecycle. Penetration testing is mentioned as an essential part of security auditing. Cybersecurity testing and validation methods are not explicit in the guidance provided by Transport Canada. Transport Canada provides tier 1 and 2 automotive suppliers with a self-assessment tool: the Vehicle Cybersecurity Assessment Tool (VCAT). The VCAT is a self-assessment questionnaire applicable for all vehicle types with varying levels of connectivity and automated features. The self-assessment questionnaire assists with evaluating the cybersecurity performance and resilience of vehicles and vehicular components. The VCAT will provide a score, measuring cybersecurity posture, as well as recommendations for mitigations [45].

3.3.3. Europe

The European Union has a diverse range of regulatory initiatives for cybersecurity of the digital marketplace, which impact upon automotive product development. The EU Cybersecurity Act (CSA) is the predominant form of regulation for cybersecurity in the EU market. Among the range of important initiatives, the CSA establishes a framework for certification of ICT products for cybersecurity called the Common Criteria-based European Candidate Cybersecurity Certification scheme (EUCC). The aim of the scheme is to enable, for the consumer, transparency and awareness of the level of assurance for cybersecurity of a digital product. The EUCC is still in development and its impact on the automotive sector is yet to be detailed [46].

The EU Cyber Resilience Act (CRA) [47] is currently being developed. This regulation will focus on providing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products and ancillary services. The CRA regulation envisages a process for the digital product cybersecurity assurance where essential baseline security requirements are defined, which can be applied selectively according to a risk management assessment of a device's intended use, considering the ecosystem or

"operational environment" in which the device will be placed. The products to be governed by the CRA include [47]:

- Connected product: A finished product that is intended to communicate directly or indirectly over the internet.
- Finished product: A product usable for its intended functions without being embedded or integrated into any other product. Components of a device, such as a processor or a sensor, should be outside the scope as security functionalities need to be assessed holistically.

In the public submissions to the CRA regulation, automotive industry bodies (European Automobile Manufacturers' Association, European Association of Automotive Suppliers, TÜV Association) pointed to other existing legislation as impacting automotive cybersecurity [47]:

- Type-approval: UN R155 and 156
- Radio Equipment Directive (2014/53/EU) and its delegated act (2022/30) (For Connected Vehicles)
- NIS 2 Directive (2020/0359(COD))

As the EU CSA is in policy implementation phase and the EU CRA is in policy conception phase, there is a sparsity of detail as to how automotive technologies will be validated and verified for cybersecurity.

Germany

Governance and Implementation of Regulation and ISO/SAE 21434:2021 In Germany, the Federal Motor Transport Authority (Kraftfahrt-Bundesamt—KBA) is responsible for bringing UNECE R155 into national legislation by issuing guidance and legally binding rules for application and review of the regulation [48]. This application document specifies testing verification procedures by document review, as well as functional security and penetration testing of a technical service (e.g., TÜV) under witness/supervision of a neutral party (KBA or an authorized body).

National Initiatives With Regard to Automotive Product V&V Testing As the EU CSA is in policy implementation phase and the EU CRA is in policy conception phase, there is a sparsity of detail as to how automotive technologies will be validated and verified for cybersecurity.

Germany Governance and Implementation of Regulation and ISO/SAE 21434:2021 In Germany, the Federal Motor Transport Authority (Kraftfahrt–Bundesamt—KBA) is responsible for bringing UNECE R155 into national legislation by issuing guidance and legally binding rules for application and review of the regulation [48]. This application document specifies testing verification procedures by document review, as well as functional security and penetration testing of a technical service (e.g., TÜV) under witness/supervision of a neutral party (KBA or an authorized body).

National Initiatives With Regard to Automotive Product V&V Testing The Quality Management Center (QMC) of the German Association of the Automotive Industry (Verband der Automobilindustrie—VDA) issued a supplement to the process management specification Automotive SPICE (Software Process Improvement and Capability Determination), which conforms with ISO 15504 [7]. This supplement, called Automotive SPICE for Cybersecurity Engineering [49], defined a set of process steps dedicated to cybersecurity engineering that is to be used in conjunction with the current Automotive SPICE process; namely:

- SEC.1 Cybersecurity Requirements Elicitation
- SEC.2 Cybersecurity Implementation
- SEC.3 Risk Treatment Verification
- SEC.4 Risk Treatment Validation, and a new management step
- MAN.7 Cybersecurity Risk Management, as well as expanding the acquisition step
- ACQ.2 Supplier Request and Selection—In particular, the risk treatment verification prescribes a specification that is suitable to provide evidence for compliance with the security requirements and the design implementation and component integration is to be tested using defined test cases (according to a verification strategy that is derived from the requirements and implementation). The corresponding best practices provides hints on what to test:
  - Requirements-based testing and interface testing on system and software level,
  - Check for any unspecified functionalities,
  - Resource consumption evaluation,
  - Control flow and data flow verification, and
  - Static analysis; for software: static code analysis, e.g., industry-recognized security-focused coding standards. As well as some testing techniques (non-exhaustive)
  - Network tests simulating attacks (non-authorized commands, signals with wrong hash key, flooding the connection with messages, etc.), and
  - Simulating brute force attacks,
  - Audits,
  - Inspections,
  - Peer reviews,
  - Walkthroughs,
  - Code reviews.

Test cases could be derived by:

- Requirements analysis,
- Building equivalence classes,
- Testing edge cases (boundary values),

- Experience-based testing. The specification also proposes to establish bidirectional traceability between the verification activities and the system design. Analogously, the risk treatment has to be validated, which means the adequacy of the implemented measures (whereas the verification assures the compliance of the measures with the requirements). The validation includes activities to also detect priorly unidentified vulnerabilities (e.g., through penetration testing), while the methodology is similar to the verification.

France

Governance and Implementation of Regulation and ISO/SAE 21434:2021 In 2021, the French legislature incorporated UNECE R155 & 156. The regulatory environment in France is conducive of close cooperation with the EU. The Ministère de la Transition écologique et solidaire is the supervising authority responsible for vehicle type approval. Association Française de Normalisation (AFNOR) is responsible for automotive standardization, including cybersecurity standards. The Agence nationale de la sécurité des systèmes d'information (ANSSI) is the primary agency responsible for cyber expertise and its role involves monitoring the cyber threat landscape, raising awareness of the necessary protections required in the digital environment of France through best practices and standardization and providing technical advice and assistance including cyber incident response through CERT France (CERT-FR) [50]. Among numerous measures contained in the Critical Information Infrastructure Law 2013, ANSSI can impose technical and organizational requirements for security and trigger audits. Recent domestic legislative updates in France reflect the widespread adoption in the EU of the EU Cybersecurity Act and other related measures [51].

National Initiatives With Regard to Automotive Product V&V Testing The French Ministry of the Interior (Ministère de l'Intérieur) issued a position paper on automated driving (L'automatisation des véhicules) [52] that contains an annex covering cybersecurity (Annexe 9: la Cybersécurité). Regarding testing, this annex contains the notion to use risk analyses, compliance audits, and penetration tests. The ANSSI states in an analysis of contributions for a—generic, but also including vehicles—cybersecurity certification scheme for the usage of static source code analysis tools, vulnerability scanners, automation of configuration audit, and protocol fuzzers for verification [53], which is, however, a very high-level recommendation.

United Kingdom

Governance and Implementation of Regulation and ISO/SAE 21434:2021 Department of Transportation (DfT) and British Standardization Organization (BSI) are the main entities in the United Kingdom toward the regulation and standardization of the automotive cybersecurity, including the cybersecurity for connected and autonomous vehicles (CAVs). DfT accommodates a center called "Centre for Connected and Autonomous Vehicles," which serves also as a part of Department for Business, Energy & Industrial Strategy. The center conducts research and publishes documents regarding the safety and security of CAVs. The Centre for the Protection of National Infrastructure (CPNI) is another entity that contributed on the research for security of CAVs [54]. In 2017, DfT, CPNI, and Centre for Connected and Autonomous Vehicles published a guidance document [54], which explained the cybersecurity needs of automotive industry in eight principles. In 2021, BSI published a white-paper [55], which defines the cybersecurity threat vectors for connected vehicles and how to meet the compliance requirements defined by the ISO/SAE 21434:2021. The paper includes an overview of ISO/SAE 21434:2021 and BSI's E2E automotive cybersecurity model, which is compliant to a set of international standards including ISO/SAE 21434:2021.

BSI PAS 1885:2018 [12] is a standards document that details the fundamental principles of cybersecurity across the vehicle's lifetime. The document provides principles that focus on organizational management of cybersecurity risks, management of the supply chain, third parties and subcontractors, and recommendations for cybersecurity design, resilience, and response measures. Principle 6, "The security of all software is managed throughout its lifecycle," prescribes a list of recommendations for testing and evaluation of vehicular software. In summary, the recommendations are:

- Open source or third-party software should be reviewed for vulnerabilities using formal code inspection reviews. Automated tools should be used to analyze the structure and security of the code.
- Configuration and management control should include evidence of testing, including test scenarios and results. Also, unresolved test defects, deficiencies, and anomalies should be documented.
- Updates shall be tested.

There is also an effort put by the British government toward the adaptation of CAVs. In 2019, the Centre for Connected and Autonomous Vehicles has started a program, called CAVPASS, in order to implement standardization, testing, and monitoring processes to ensure the resilience of CAVs against cyberattacks [56]. Zenzic is another organization founded by the government and industry in order to embrace the cybersecurity and safety challenges brought by the Connected and Autonomous Mobility (CAM). The organization published a feasibility report in 2020 [57], which stated the outcomes of several projects. The report included a part regarding the measurement and monitoring the cyber resilience, mentioning the digital twin technology for validation, assurance, and certification of CAVs.

4. Processes and Tools Used in The Industry

In order to examine which processes and tools are used in the industry, we issued questionnaires to experts in the field,

consisting of members of OEMs, suppliers, and automotive engineering companies. The questions targeted in collecting common practices on what is to be tested (test targets), how to test (standards usage, test types, and test derivation), and how to support the testing (test tools).

4.1. Test Targets

E/E components remain the predominant areas of focus for SUT due their importance for functionality of the vehicle. Due to the preponderance of connected vehicular technologies, communication protocols are an area of concentric concern for cybersecurity testing. Emerging SUTs include the end-to-end driving technology which supports autonomous-assisted and autonomous driving. Third-party service providers for verification and validation are popularly used due to their existing experience of testing and certification, alignment with ISO/SAE 21434:2021 and other standards which emphasize the use of third parties for independent verification and validation, and lack of available skills for cybersecurity testing of automotive products. A majority of respondents answered that they have an established interface agreement for cybersecurity testing. Most OEMs follow a document-based audition process in their verification and validation agreement.

4.2. Standards Utilization

Overwhelmingly, ISO/SAE 21434:2021 is used for cybersecurity verification and validation. Respondents also mentioned well-established, complimentary standards such as ISO/IEC 15408 (Common Criteria) and ISO/IEC 27034 (Application Security Standards). The testing process for SUTs are mainly conducted on a case-by-case basis. The limited use of test matrix and standard test sets can be seen as due to a variety of reasons including repeatable test processes cannot be ubiquitously applied to diverse range of automotive technologies, level of integration, and architecture requires testing to be approached on a case-by-case basis, lack of development, and adoption of testing metrics and criteria, cybersecurity testing is still developing and there is a lack of adoption of testing processes that support automation and repeatable testing. OEMs conduct functional testing, vulnerability scanning, penetration testing, and fuzz testing. All of these test procedures are recommendations of ISO/SAE 21434:2021 and are essential as part of an automotive cybersecurity testing program. Specifications coverage is the most popular method to measure and maximize test coverage of the SUT. This aligns with product development lifecycle and the focus on assurance for the intended functionality of the automotive component. Emerging methods include considerations for the requirements from UN R155.

4.3. Types of Testing

Our survey results show that our respondents practice various types of testing during different stages of their development lifecycle. These are (1) fuzzing, (2) penetration testing, and (3) functional testing. This section compiles these methods by describing and referring to the phases of development that each type of testing utilized. We also give further detail by adding other methods that are applicable for automotive cybersecurity testing, which are found in the literature. These are (3) model-based security testing, (4) risk-based security testing, and (6) vulnerability scanning.

Fuzzing: Fuzzing, or fuzz testing, refers to subjecting the software system (or components individually) to a large volume of invalid, unexpected, or random inputs that are known as "fuzz." By exposing the executable software to a wide range of invalid data, vulnerabilities can be identified that are not known previously. To generate a variety of inputs that can lead the program to failure, which is a difficult process to cover all cases, there are several techniques used. One of them is to generate the input data based on the analysis of a program's coverage, behavior, and source code, another is to implement mutation techniques on the generated data according to the program's feedback from the previously fed data, or to randomly generate [58]. Fuzzing is conducted during the development and testing phases of ECUs and infotainment systems to discover vulnerabilities, software bugs, or unexpected behavior that may lead to failures.

Penetration Testing: Penetration testing is conducted to assess the security of the hardware, software, and communication systems, by mimicking real-world security attacks on the subject. It involves actively scanning and exploiting vulnerabilities in the system with methods such as injection and tampering to determine its susceptibility to unauthorized access, data breaches, or malicious activities. Penetration testing is performed during the entire development lifecycle and before deployment to identify security flaws and mitigate them before they can be exploited by attackers.

SAE J3061 and o ISO/SAE 21434 state the necessity of penetration testing and it is included as part of the best practices document published by Auto ISAC [43]. Also, a recent study [59] shows its wide usage among security testing types. It is also seen that, among different knowledge levels, black-box testing is the most preferred one for penetration testing.

Functional Security Testing: Focuses on evaluating the security features and mechanisms of the system to ensure they function as intended. It involves subjecting security properties, such as authentication, authorization, encryption, and secure communication mechanisms to test and verify their compliance with the security requirements and validate the behavior. This type of testing is applicable by both software-in-the-loop and hardware-in-the-loop testbeds, which may be utilized throughout the development [60]. Functional security testing can be conducted throughout the development lifecycle and pre-deployment stage to verify and validate the security features.

Model-based Security Testing: Model-based security testing involves creating formal or semi-formal models of a feature, and using these models to perform security analysis and verification of conformity to requirements. Models can be security properties (i.e., confidentiality, integrity, authentication, etc.), vulnerabilities, and security safeguards that are

being designed for the overall system, and also threats and attacks to the system [61]. This type of testing helps identify potential security weaknesses in the design and earlier phases of the development lifecycle and enables engineers to mitigate the vulnerabilities by designing robust features.

Risk-based Security Testing: Focuses on assessing the security of a system based on the potential security risks and their impact. This type of testing is based on threat analysis and risk assessment (TARA) techniques to prioritize the most critical assets, threats, and vulnerabilities for allocating testing resources accordingly [59]. Risk-based security testing considers the likelihood of an attack, its potential impact on the system, and the value of the assets at risk. It is performed throughout the development lifecycle to ensure most critical security risks are addressed.

Vulnerability Scanning: This is a systematic process to test the system for known vulnerabilities that can be exploited by known threats. This type of testing can target the source code by conducting either static or dynamic analysis to understand whether the software poses vulnerabilities due to memory usage or the interfaces for discovering unprotected entries (i.e. port scanning) [60]. Automated tools and scripts are used in this approach so that they can be implemented as part of the DevOps cycle to conduct regular and repeatable tests with each increment, during development, and after deployment (i.e., for updated software).

Two-thirds of respondents confirmed that they utilize functional testing and penetration testing within their verification and validation processes, which support the entire automotive development lifecycle. Validation activities were conducted close to the end of the product development phase and before release for post-development and consisted of analysis and testing. Verification activities were conducted during the concept and product development phase and consisted of review, analysis, and multiple rounds of penetration testing. One-third of respondents have not yet adopted the cybersecurity verification and validation processes of the ISO/SAE 21434:2021 standard.

4.4. Test Derivation

There is a couple of ways to derive test cases from a performed asset/security analysis: based on derived requirements from a model (e.g., a TARA, cf. previous section) that could also be subject to model checking; based on specifications (both standards and vendor specifications), based on the structure (i.e., the architecture—e.g., tests that verify the correctness of a security gateway's functioning), based on the experience of the respective penetration tester (i.e., trusting the right test cases to be designed to expert knowledge), or based on known faults. The respondents roughly evenly perform requirements, specification, and experience-based test derivation, while structure-based tests are significantly less (one-third) used, information is UNECE's Regulation 155 (see above in the respective section) [1]. In its Annex 5 it defines a catalogue of countermeasures that can serve as requirements that might be verified by testing. Regarding the testing methods, it is equally proliferated to use white box (full access to information about the SUT), black box (just the SUT "as is," with no additional information), and gray box (some information, mainly handbooks, API documentation, etc.) approaches. Only a minority (one-third) of the respondents claimed that they use a baseline for testing. This means a minimum set of tests generically issued to all of their SUTs, regardless of their nature. The relative majority of those uses testing the requirement specification followed by using prepared test plans, test cases, and test data and, lastly, testing the design specification and predefined generic tests for the source code itself. One specific test set mentioned is testing all wireless and wired interfaces (e.g., OBD) for their susceptibility to act as an entry vector into the vehicle.

4.5. Test Tool Categories

Respondents use a diverse range of commercial-off-the-shelf (COTS), open-source (OS), customized, and in-house (internally developed) tools in their penetration testing activities. The results show a bias toward COTS and OS tools. The respondents also identified a number of tools that were used to test recent high-profile vulnerabilities such as Blueborne (a well-known Bluetooth attack) and ROCA (cryptographic weakness). With the emphasis ISO/SAE 21434:2021 places on TARA, it is apparent that automotive cybersecurity testers are agile in developing and utilizing toolsets to keep pace with the dynamic threat environment. Table 2 categorizes specifically mentioned tools. When asked for specific tools during the phases of an attack test—pre-attack (scanning, CAN analysis, etc.), attack (exploit frameworks, etc.), and post-attack (reporting, life cycle management)—respondents answered with a variety of tools.

Table 3 provides an overview of some commonly used tools, displaying the phase that are used in reconnaissance, attack, or life cycle governance; the tool category (cf. Table 2); and the area of testing (IP/web, wireless, and in-vehicle networks as well as reverse engineering). In that context, IP Network/web testing tools refer to tools originally used in traditional IT testing, targeting network, and web-based interfaces. Currently, they are ordinarily used mainly to perform tests in automotive ethernet or on targets that have interfaces similar to traditional IT systems, e.g., infotainment head units running on an Android operating system. Wireless Automotive refers to tools to assess implementations of wireless protocol stacks that are popular in the automotive industry, most prominently Bluetooth and WiFi. In-vehicle network (IVN) tools mainly refer to tools for testing CAN bus and Automotive Ethernet environments. Lastly, reverse engineering tools are used to scrutinize binaries of automotive control systems and search for potential weaknesses inside the code by following control flows. The other axis of the table shows whether the tool is considered to be more in reconnaissance (information gathering) or attack (actual intrusion) phase of cracking a system, as well as life cycle management tools that support the security governance and help in planning tests throughout a system's life cycle.

TABLE 2 Tool categories.

Tool category	Description	Automotive test usage
Vulnerability assessment	Enables performance of a scan of a device or information system to discover vulnerability of the target system to known vulnerabilities.	Nmap and Nessus could be used to find open communication ports on an infotainment head unit and its vulnerabilities.
Web application	Enables analysis of the codebase of web applications and mobile device applications.	Predominantly used in the testing of infotainment systems and customer applications.
Reverse engineering	Used for analyzing the binary code of the software to identify vulnerabilities (due to memory usage, logic, etc.). Tools such as IDA and Volatility (see Table 3) are used for data extraction for analysis.	
Protocol analysis	Enables analysis of protocols to understand the architecture and identify vulnerabilities.	Used for internal (CAN, LIN, MOST, FlexRay) and external (Wireless, Radio, Bluetooth) networks.
Fuzzing	Used to assess the security of a system to unsanitized data input. This can be either randomized or targeted unsanitized data input. It is popularly used in software engineering to identify bugs in the codebase.	Fuzzing is used ubiquitously from the embedded hardware ECUs to the infotainment system, mostly through customized or in-house tools aligned with the OEM software development processes.

5. Discussion

The most influential document is arguably UNECE R155 for its normative and legally binding character. This document contains a list of requirements (in an annex) that could serve as test targets. Further details are specified on a national level, as is the details of the mandated CSMS. The specification of such a system is found in ISO 21434:2021. Both documents, however, specify testing requirements at a very high level. Therefore, the ISO maintains ongoing efforts to specify test classifications, as well as V&V procedures in more detail, giving guidance for testing. As the UNECE must be adopted into national regulations, the concrete embodiments differ. Nonetheless, it is common that the level of detail is coarse, leaving much room for interpretation open for implementers. Regional standards are likewise high-level descriptive in general, focusing on engineering process topics. An exception are some standards specifically from the Asian area that give fine-grained descriptions for test procedures for single components. The research of regional standards showed no clear bias in testing procedures by region, although the underspecification leaves room for interpretation differences by both different regional authorities and implementers. What is missing globally is test implementation details for systems at vehicle level. The reason, drawn out of expert interviews, is the early stage maturity of the topic. First, details for many of the components have to emerge, before they can be tied to high-level test procedures at vehicle level. To perform testing and analysis, most

TABLE 3 Testing tools per attack phase, type, and category.

Phase	Tool	IP network/web	Wireless automotive	IVN	Reverse engineering	Tool category
Reconnaissance	Nessus	✓				Vulnerability assessment
	Nmap	✓				Vulnerability assessment
	Dirbuster	✓				Fuzzing
	Bluescanner		✓			Vulnerability assessment
	Wireshark	✓				Protocol analysis
	GNU Radio Companion		✓			Protocol analysis
	Universal Radio Hacker		✓			Protocol analysis
	CANoe			✓		Protocol analysis
Attack tools	Ghidra				✓	Reverse engineering
	Android Studio				✓	Reverse engineering
	Aircrack Suite		✓			Vulnerability assessment
	URH		✓			Reverse engineering
	Volatility				✓	Reverse engineering
	Genymotion				✓	Protocol analysis
	IDA				✓	Reverse engineering
	Burpsuite	✓				Web application
	American Fuzzy Lop				✓	Fuzzing
LCM	PTC Integrity					

players currently use general-purpose tools that are proliferated in IT security testing (e.g., fuzzers, reverse engineering, and protocol analysis tools), as well as specialized hard- and software for automotive systems (particularly CAN buses). These tools are used primarily in a manual testing process. There is few automatic test generation and execution methodology for automotive security (such as [62]). Apart from systems for supporting the testing process by automating tasks (e.g., vulnerability scanning) and embedding this in an automated toolchain, one trend tends to be going toward model-based testing.

6. Conclusion

This research provided an overview of international and regional standards and found that the current state-of-the-art lacks proscribed detail of V&V procedures that would enable alignment within different regions and industry. The developmental nature of V&V testing was further highlighted by the industry working group responses, which demonstrated that traditional enterprise information technology and processes were used. We see, however, that there is considerable development in this area with industry identifying connected and autonomous vehicle technologies as increasing in priority for testing and the focus on developing toolsets for automotive cybersecurity testing. Furthermore, we also see a concentration of effort by national authorities to enshrine UN R.155 into the national regulatory frameworks for vehicle regulation and advocate for best practice guidelines such as those in ISO/SAE 21434.

As the UNECE regulation and its accompanying traits are fairly new (first effective only in mid-2022), there is a significant lack of experience on necessary test procedures. Practical advice will emerge in greater detail when it could be clarified how the legislation is actually handled. The same applies for standards, as pivotal initiatives (e.g., from ISO) are still in a very early project phase—with forthcoming of these endeavors more detailed specifications can be given. Dedicated, automated toolchains will follow that trail, so far incipient stages are given.

Acknowledgments

This work has been supported by the European Commission through the H2020 teaming project Finest Twins (grant No. 856602) and European Union's Horizon 2020 Research and Innovation Programme, under grant agreement No 883321 (CitySCAPE). The authors want to thank the International Alliance for Mobility Testing and Standardization (IAMTS) for their support while writing this article.

Contact Information

Stefan Marksteiner
Corresponding author
stefan.marksteiner@avl.com

References

1. United Nations Economic and Social Council—Economic Commission for Europe, "Cyber Security and Cyber Security Management System," Regulation 155, Brussels, 2021.
2. SAE International, "J3061-2 (WIP) Security Testing Methods," accessed June 28, 2023, https://www.sae.org/standards/content/j3061-2/; International Organization for Standardization and Society of Automotive Engineers, "Road Vehicles—Cybersecurity Engineering," ISO/SAE Standard 21434:2021, 2021.
3. Schmittner, C. and Macher, G., "Automotive Cybersecurity Standards—Relation and Overview," in *Computer Safety, Reliability, and Security: SAFECOMP 2019 Workshops, ASSURE, DECSoS, SASSUR, STRIVE, and WAISE, Turku, Finland, September 10, 2019, Proceedings*, Romanovsky, A., Troubitsyna, E., Gashi, I., Schoitsch, E. et al. (Eds.) (Berlin, Heidelberg: Springer-Verlag, 2019), 153-165, https://doi.org/10.1007/978-3-030-26250-1_12.
4. Macher, G., Schmittner, C., Veledar, O., and Brenner, E., "ISO/SAE DIS 21434 Automotive Cybersecurity Standard—In a Nutshell," in *Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops*, Casimiro, A., Ortmeier, F., Schoitsch, E., Bitsch, F. et al. (Eds.) (Cham: Springer International Publishing, 2020), 123-135.
5. International Organization for Standardization and Society of Automotive Engineers, "Road Vehicles—Cybersecurity Engineering," ISO/SAE Draft International Standard DIS 21434, 2021.
6. Schober, T. and Griessnig, G., "Cybersecurity Regulations and Standards in the Automotive Domain," in *Systems, Software and Services Process Improvement (Communications in Computer and Information Science)*, Yilmaz, M., Clarke, P., Messnarz, R., and Wöran, B. (Eds.) (Cham: Springer International Publishing, 2022), 530-539, https://doi.org/10.1007/978-3-031-15559-8_38.
7. International Organization for Standardization, "Information Technology—Process Assessment—Part 5: An Exemplar Software Life Cycle Process Assessment Model," ISO/IEC Standard 15504-5, 2012.
8. Society of Automotive Engineers, "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," SAE Standard J3061_202112, 2021.
9. United Nations Economic and Social Council—Economic Commission for Europe, "Software Update and Software Update Management System," Regulation 156, Brussels, 2021.
10. United Nations Economic and Social Council—Economic Commission for Europe, "UN Regulation on Uniform Provisions Concerning the Approval of Vehicles With Regard to Cyber Security and of Their Cybersecurity Management Systems," Technical Report ECE/TRANS/WP.29/2020/79, Brussels, 2020.
11. National Highway Traffic Safety Administration, "Cybersecurity Best Practices for the Safety of Modern Vehicles (Draft Update 2020)," Draft Update of DOT HS 812 333, Washington, DC, 2020.

12. British Standards Institution, "The Fundamental Principles of Automotive Cyber Security—Specification," BSI PAS 1885:2018, 2018.
13. Hu, S., Chen, Q.A., Sun, J., Feng, Y. et al., "Automated Discovery of Denial-of-Service Vulnerabilities in Connected Vehicle Protocols," in *30th USENIX Security Symposium (USENIX Security 21)*, USENIX Association, Vancouver, Canada, 2021, 3219-3236, https://www.usenix.org/conference/usenixsecurity21/presentation/hu-shengtuo.
14. Shen, J., Won, J.Y., Chen, Z., and Chen, Q.A., "Drift with Devil: Security of Multi-Sensor Fusion Based Localization in High-Level Autonomous Driving under GPS Spoofing," in *Proceedings of the 29th USENIX Security Symposium (2020)*, Boston, MA, 2020, 931-948.
15. Sun, J., Cao, Y., Chen, Q.A., and Morley Mao, Z., "Towards Robust LiDAR-Based Perception in Autonomous Driving: General Black-Box Adversarial Sensor Attack and Countermeasures," in *Proceedings of the 29th USENIX Security Symposium (2020)*, Boston, MA, 2020, 877-894, arXiv:2006.16974.
16. Kim, H., Ozgur Ozmen, M., Bianchi, A., Berkay Celik, Z. et al., "PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles," in *Network and Distributed System Security Symposium (NDSS)*, Virtual, 2021, 1-18, https://beerkay.github.io/papers/Berkay2021PGFuzzNDSS.pdf.
17. Kim, T., Kim, C.H., Rhee, J., Fei, F. et al., "RVFuzzer: Finding Input Validation Bugs in Robotic Vehicles through Control-Guided Testing," in *28th USENIX Security Symposium (USENIX Security 19)*, USENIX Association, Santa Clara, CA, 2019, 425-442, https://www.usenix.org/conference/usenixsecurity19/presentation/kim.
18. Vinzenz, N. and Oka, D.K., "Integrating Fuzz Testing into the Cybersecurity Validation Strategy," SAE Technical Paper 2021-01-0139 (2021), doi:https://doi.org/10.4271/2021-01-0139.
19. Ebrahimi, M. et al., "A Systematic Approach to Automotive Security," in *Formal Methods*, Lecture Notes in Computer Science, Chechik, M., Katoen, J.-P., and Leucker, M. (Eds.) (Cham: Springer International Publishing, 2023), 598-609, doi:10.1007/978-3-031-27481-7_34.
20. Oka, D., "Fuzz Testing Virtual ECUs as Part of the Continuous Security Testing Process," *SAE Int. J. Transp. Cyber. & Privacy* 2, no. 2 (2020): 159-168, doi:https://doi.org/10.4271/11-02-02-0014.
21. United Nations Economic and Social Council—Economic Commission for Europe, "Agreement Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations," ECE/TRANS/WP.29/343/Rev. 30, 2022, 43.
22. The Ministry of Industry and Information Technology of China (MIIT), "Opinions of the Ministry of Industry and Information Technology on Strengthening the Management of Smart Connected Automobile Manufactures and Product Permit," MIIT Equipment Industry 103, 2021.
23. The Ministry of Industry and Information Technology of China (MIIT), "Suggestions on Strengthening the Type Approval Management of Intelligent & Connected Vehicle Manufacturers and Products," MIIT 5, 2021.
24. National Technical Committee of Auto Standardization, "General Technical Requirements for Vehicle Cybersecurity," GB/T 40861–2021, 2021.
25. The Ministry of Industry and Information Technology of China (MIIT), "Notice of the Ministry of Industry and Information Technology on Strengthening the Cyber Security and Data Security of Internet of Vehicles," MIIT Cybersecurity 134, 2021.
26. The Ministry of Industry and Information Technology of China (MIIT), "Security Technical Requirements for Connected Vehicle Based on Public Telecommunication Network," YD/T 3737-2020, 2020.
27. Chinese National Information Security Standardization Technical Committee, "Information Security Technology—Cybersecurity Technical Requirements for In-Vehicle Network Equipment," Technical Report, 2020.
28. Chinese National Information Security Standardization Technical Committee, "Technical Requirements for Cybersecurity of Electric Vehicles Charging System (Draft for Comments)," GB/T, 2020.
29. Chinese National Automotive Standardization Technical Committee, "Technical Requirements and Test Methods for Cybersecurity of Remote Service and Management System for Electric Vehicles," GB/T, 2021.
30. Japanese Ministry of Land, Infrastructure, Transport and Tourism Automobile Bureau, "Safety Technical Guidelines for Self-Driving Vehicles," Technical Report, 2018.
31. Information-Technology Promotion Agency, Japan, "Approaches for Vehicle Information Security," Technical Report, 2013.
32. Japan Automotive Software Platform and Architecture (JASPAR), "About Us," accessed November 10, 2023, https://www.jaspar.jp/en/about_us.
33. Ministry of Land, Infrastructure and Transportation, "Approach of Republic of Korea Harmonizing the UN Regulation No. 155," Technical Report, 2021.
34. ATIC, "Brief Analysis of the July 2022 Korean Regulatory Updates," Technical Report, 2022.
35. National Highway Traffic Safety Administration, "Understanding NHTSA's Regulatory Tools," Report, Washington, DC, 2017.
36. NHTSA, "Vehicle Cybersecurity," accessed June 28, 2023, https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity.
37. National Highway Traffic Safety Administration, "Report to Congress: 'Electronic Systems Performance in Passenger Motor Vehicles'," Technical Report, 2015.
38. McCarthy, C., Harnett, K., Carter, A., and Hatipoglu, C., "Assessment of the Information Sharing and Analysis Center Model," Technical Report DOT HS 812 076, National Highway Traffic Safety Administration, Washington, DC, 2014.

39. NHTSA, "NHTSA Seeks Comment on Cybersecurity Best Practices for the Safety of Modern Vehicles," accessed June 28, 2023, https://www.nhtsa.gov/press-releases/nhtsa-seeks-comment-cybersecurity-best-practices-safety-modern-vehicles.
40. National Highway Traffic Safety Administration, "Cybersecurity Best Practices for Modern Vehicles," Technical Report DOT HS 812 333, Washington, DC, 2016.
41. National Highway Traffic Safety Administration, "Cybersecurity Best Practices for the Safety of Modern Vehicles," Pre-Final, Washington, DC, 2022.
42. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Technical Report, Gaithersburg, MD, 2018.
43. Automotive Information Sharing and Analysis Center, "Best Practices," Technical Report, 2016.
44. Automotive Information Sharing and Analysis Center, "Best Practices—Security Development Lifecycle," Technical Report, 2020.
45. Transport Canada, "Canada's Vehicle Cyber Security Guidance," Technical Report T46-61/2020E, 2020.
46. European Union, "The EU Cybersecurity Act," Technical Report, 2020.
47. European Union, "Cybersecurity Resilience Act," Technical Report, 2022.
48. Kraftfahrt-Bundesamt, "Application of the Rules for Designation/Recognition for Technical Services (Categories A, B, D)," Technical Report, 2021.
49. VDA QMC Project Group 13, "Automotive SPICE—Process Reference and Assessment Model for Cybersecurity Engineering," Core Specification 1.0, Quality Management Center of the German Association of the Automotive Industry, 2021.
50. Ministère de la Transition écologique et solidaire, "Cybersecurity in France for Civil Aviation," Technical Report, Direction générale de l'Aviation civile, 2018.
51. Agence nationale de la sécurité des systèmes d' information, "Cybersecurity Act," accessed November 10, 2023, https://www.ssi.gouv.fr/administration/reglementation/cybersecurity-act/.
52. Rocchi, J.-F., Bodino, P., De Tréglodé, H., Flury-Hérard, B. et al., "L'automatisation Des Véhicules; Annexe No. 9: La Cyber Sécurité. Inspection Generale de l'administration 16040-R," Inspection generale de l'administration and Conseil general de l'environnement et du developpement durable, 2017.
53. Agence nationale de la sécurité des systèmes d'information, "Analyse Des Contributions Reçues Suite à l'appel à Manifestation d'intérêt Sur La Certification de Sécurité de Niveaux Substantiel et Élémentaire," Technical Report, 2019.
54. United Kingdom Department for Transport, "The Key Principles of Cyber Security for Connected and Automated Vehicles," Technical Report, 2017.
55. British Standards Institution, "Automotive Cybersecurity Insights Paper," BSI PAS, 2021.
56. "Centre for Connected and Autonomous Vehicles, "Connected and Automated Vehicles: Process for Assuring Safety and Security (CAVPASS)," accessed June 28, 2023, https://www.gov.uk/guidance/connected-and-automated-vehicles-process-for-assuring-safety-and-security-cavpass.
57. Zenzic, "Cyber Resilience in Connected and Automated Mobility (CAM)—Cyber Feasibility Report," 2020.
58. Li, J., Zhao, B., and Zhang, C., "Fuzzing: A Survey," *Cybersecurity* 1, no. 1 (2018): 6, doi:https://doi.org/10.1186/s42400-018-0002-y.
59. Luo, F., Zhang, X., Yang, Z., Jiang, Y. et al., "Cybersecurity Testing for Automotive Domain: A Survey," *Sensors* 22, no. 23 (2022): 9211.
60. Mahmood, S., Nguyen, H.N., and Shaikh, S.A., "Automotive Cybersecurity Testing: Survey of Testbeds and Methods," in: *Digital Transformation, Cyber Security and Resilience of Modern Societies*, Studies in Big Data, vol. 84, Tagarev, T., Atanassov, K.T., Kharchenko, V., and Kacprzyk, J. (Eds.) (2021), Springer, Cham, https://doi.org/10.1007/978-3-030-65722-2_14.
61. Felderer, M., Zech, P., Breu, R., Büchler, M. et al., "Model-Based Security Testing: A Taxonomy and Systematic Classification," *Software Testing Verification and Reliability* 26, no. 2 (2015): 119-148, doi:10.1002/stvr.1580.
62. Marksteiner, S., Bronfman, S., Wolf, M., and Lazebnik, E., "Using Cyber Digital Twins for Automated Automotive Cybersecurity Testing," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, Vienna, Austria, 2021, 123-128, doi:https://doi.org/10.1109/EuroSPW54576.2021.00020.